

# Microsoft Cybersecurity Architect – Flexible Training («SC100V»)

Dieses SC-100 Training besteht aus jeweils maximal 2 Halbtages-Sessions pro Woche über höchstens 4 Wochen. Klicken Sie für den Session-Plan am Ende der Seite, wo Sie Ihr gewünschtes Datum auswählen, auf «Stundenplan».

**Dauer:** 4 Tage

**Preis:** 3'400.- zzgl. 8.1% MWST

**Kursdokumente:** Offizielle Microsoft-Unterlagen und Microsoft Learn

**Herstellercode:** SC-100

## Inhalt

Der Inhalt dieses Flexible Training leitet sich aus der Prüfung «[SC-100: Microsoft Cybersecurity Architect](#)» ab. Beginnen Sie schon jetzt auf Microsoft Learn mit der Vorbereitung auf den Kurs und nutzen Sie den Learning Support, wenn Sie Fragen haben. Während der jeweiligen 3h-Trainer-Sessions arbeiten Sie mit den offiziellen Microsoft-Kursunterlagen (mehr Informationen unter «Methodik & Didaktik»).

Dieser Kurs bereitet die Teilnehmer darauf vor, Cybersicherheits-Strategien in den folgenden Bereichen zu entwerfen und zu bewerten: Zero Trust, Governance Risk Compliance (GRC), Security Operations (SecOps) sowie Daten und Anwendungen.

### Modul 1: Aufbau einer umfassenden Sicherheitsstrategie und -architektur

#### Lektionen

- Überblick über Zero Trust
- Entwicklung von Integrationspunkten in einer Architektur
- Entwicklung von Sicherheitsanforderungen auf der Grundlage von Geschäftszielen
- Übersetzen von Sicherheitsanforderungen in technische Fähigkeiten
- Sicherheit für eine Ausfallsicherheitsstrategie entwickeln
- Entwurf einer Sicherheitsstrategie für hybride und mandantenfähige Umgebungen
- Entwurf von technischen und Governance-Strategien für die Filterung und Segmentierung des Datenverkehrs
- Verstehen der Sicherheit von Protokollen
- **Übung: Aufbau einer umfassenden Sicherheitsstrategie und -architektur**

### Modul 2: Entwurf einer Strategie für Sicherheitsoperationen

#### Lektionen

- Verstehen von Rahmenwerken, Prozessen und Verfahren für den Sicherheitsbetrieb
- Entwerfen einer Sicherheitsstrategie für Protokollierung und Auditing
- Entwicklung von Sicherheitsabläufen für hybride und Multi-Cloud-Umgebungen
- Entwerfen einer Strategie für Security Information and Event Management (SIEM) und Security Orchestration,
- Bewertung von Sicherheitsabläufen
- Überprüfung von Sicherheitsstrategien für das Incident Management
- Bewertung der Strategie für den Sicherheitsbetrieb zum Austausch technischer Bedrohungsdaten
- Quellen für Erkenntnisse über Bedrohungen und Abhilfemassnahmen überwachen

### Modul 3: Entwurf einer Strategie für die Identitätssicherheit

#### Lektionen

- Den Zugang zu Cloud-Ressourcen sichern

- Einen Identitätsspeicher für die Sicherheit empfehlen
- Sichere Authentifizierungs- und Sicherheitsautorisierungsstrategien empfehlen
- Sicheren bedingten Zugriff
- Eine Strategie für Rollenzuweisung und Delegation entwerfen
- Definition von Identity Governance für Zugriffsüberprüfungen und Berechtigungsmanagement
- Entwurf einer Sicherheitsstrategie für den Zugriff privilegierter Rollen auf die Infrastruktur
- Entwurf einer Sicherheitsstrategie für privilegierte Aktivitäten
- Verstehen der Sicherheit von Protokollen

#### **Modul 4: Bewertung einer Strategie zur Einhaltung von Vorschriften**

##### **Lektionen**

- Interpretieren der Compliance-Anforderungen und ihrer technischen Möglichkeiten
- Bewertung der Konformität der Infrastruktur mithilfe von Microsoft Defender for Cloud
- Interpretieren von Konformitätsbewertungen und Empfehlen von Massnahmen zur Behebung von Problemen oder zur Verbesserung der Sicherheit
- Entwurf und Validierung der Implementierung von Azure-Richtlinien
- Design für Datenresidenz Anforderungen
- Übersetzen von Datenschutzerfordernissen in Anforderungen für Sicherheitslösungen

#### **Modul 5: Bewertung der Sicherheitslage und Empfehlung technischer Strategien zur Risikoverwaltung**

##### **Lektionen**

- Bewerten der Sicherheitslage mit Hilfe von Benchmarks
- Bewerten der Sicherheitslage mithilfe von Microsoft Defender for Cloud
- Bewertung der Sicherheitslage mit Hilfe von Secure Scores
- Bewertung der Sicherheitshygiene von Cloud-Workloads
- Sicherheit für eine Azure Landing Zone entwerfen
- Interpretation technischer Bedrohungsdaten und Empfehlung von Risikominderungsmaßnahmen
- Empfehlung von Sicherheitsfunktionen oder -kontrollen, um identifizierte Risiken zu mindern

#### **Modul 6: Verstehen von Best Practices für die Architektur und wie sie sich durch die Cloud verändern**

##### **Lektionen**

- Eine Sicherheitsstrategie teamübergreifend planen und umsetzen
- Eine Strategie und einen Prozess für die proaktive und kontinuierliche Weiterentwicklung einer Sicherheitsstrategie einrichten
- Verstehen von Netzwerkprotokollen und bewährten Verfahren zur Netzwerksegmentierung und Verkehrsfilterung

#### **Modul 7: Eine Strategie zur Sicherung von Server- und Client-Endpunkten entwerfen**

##### **Lektionen**

- Festlegen von Sicherheitsgrundlagen für Server- und Client-Endpunkte
- Festlegen von Sicherheitsanforderungen für Server
- Festlegen von Sicherheitsanforderungen für mobile Geräte und Clients
- Festlegen der Anforderungen für die Sicherung von Active Directory-Domänendiensten
- Entwerfen einer Strategie zur Verwaltung von Geheimnissen, Schlüsseln und Zertifikaten
- Entwerfen einer Strategie für sicheren Fernzugriff
- Verstehen von Rahmenwerken, Prozessen und Verfahren für Sicherheitsoperationen
- Tiefgreifende forensische Verfahren nach Ressourcentyp verstehen

## Modul 8: Entwerfen einer Strategie zur Sicherung von PaaS-, IaaS- und SaaS-Diensten

### Lektionen

- Festlegen von Sicherheitsgrundlagen für PaaS-, IaaS- und SaaS-Dienste
- Festlegen der Sicherheitsanforderungen für IoT-, Daten-, Web- und Speicher-Workloads
- Festlegen von Sicherheitsanforderungen für Container und Container-Orchestrierung

## Modul 9: Spezifizieren von Sicherheitsanforderungen für Anwendungen

### Lektionen

- Verstehen der Modellierung von Anwendungsbedrohungen
- Festlegen von Prioritäten für die Eindämmung von Bedrohungen für Anwendungen
- Einen Sicherheitsstandard für das Onboarding einer neuen Anwendung spezifizieren
- Festlegen einer Sicherheitsstrategie für Anwendungen und APIs

## Modul 10: Entwerfen einer Strategie zur Sicherung von Daten

### Lektionen

- Prioritäten für die Abschwächung von Bedrohungen für Daten festlegen
- Eine Strategie zur Identifizierung und zum Schutz sensibler Daten entwerfen
- Festlegen eines Verschlüsselungsstandards für ruhende und bewegte Daten

## Key Learnings

- Entwurf einer Zero-Trust-Strategie und -Architektur
- Bewertung der technischen Strategien für Governance Risk Compliance (GRC) und der Strategien für den Sicherheitsbetrieb
- Entwurf einer Sicherheitsstrategie für die Infrastruktur
- Ausarbeitung einer Strategie für Daten und Anwendungen

## Methodik & Didaktik

### Digicomp Flexible-Learning-Ansatz:

- **Trainings-Modalität:** Während einer Dauer von 4 Wochen finden 6-8 halbtägige (je 3h) virtuelle Live-Sessions mit unseren Azure-MCT-Experten statt. Die Sessions sind bereits geplant und lassen sich super mit dem Arbeitsalltag verbinden. Zwischen den Sessions bleibt genügend Zeit, das gelernte Wissen zu verarbeiten.
- **Detaillierter Session-Plan:** Klicken Sie dazu am Ende der Seite, wo Sie Ihr gewünschtes Datum auswählen, auf «Stundenplan».

## Zielpublikum

IT-Fachleute mit fortgeschrittenen Erfahrungen und Kenntnissen in einer Vielzahl von Bereichen der Sicherheitstechnik, einschliesslich Identität und Zugang, Plattformschutz, Sicherheitsabläufe, Datensicherheit und Anwendungssicherheit. Sie sollten auch Erfahrung mit Hybrid- und Cloud-Implementierungen haben.

## Anforderungen

- Fortgeschrittene Erfahrungen und Kenntnisse in den Bereichen Identität und Zugang, Plattformschutz, Sicherheitsabläufe, Datensicherheit und Anwendungssicherheit
- Erfahrung mit Hybrid- und Cloud-Implementierungen
- **Microsoft Identity and Access Administrator – Flexible Training («SC300V»)**
- **Microsoft Azure Security Engineer Technologies – Flexible Training («AZ500V»)**
- **Microsoft Security Operations Analyst – Flexible Training («SC200V»)**

## Zertifizierung

Dieses Flexible Training bereitet Sie vor auf:

- **Prüfung:** «SC-100: Microsoft Cybersecurity Architect» für die
- **Zertifizierung:** «Microsoft Certified: Cybersecurity Architect Expert»

## Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder [info@digicomp.ch](mailto:info@digicomp.ch). Detaillierte Infos zu den Terminen finden Sie unter [www.digicomp.ch/weiterbildung-digital-transformation-technologies/cloud/cloud-security/kurs-microsoft-cybersecurity-architect-flexible-training-sc-100](https://www.digicomp.ch/weiterbildung-digital-transformation-technologies/cloud/cloud-security/kurs-microsoft-cybersecurity-architect-flexible-training-sc-100)